IUS REVISTA DEL INSTITUTO DE CIENCIAS JURÍDICAS DE PUEBLA, MÉXICO. E-ISSN 1870-2147. NUEVA ÉPOCA VOL. 15, No. 48. JULIO - DICIEMBRE DE 2021. PP 179-207

El derecho de protección de datos personales en los sistemas de inteligencia artificial*

The personal data protection right in artificial intelligence systems

Olivia Andrea Mendoza Enríquez**

RESUMEN

El objetivo del documento es analizar la inteligencia artificial (IA) desde la visión del derecho de protección de datos personales con el fin de identificar los desafíos que existen para la salvaguarda de este derecho humano. La aportación se desarrolla a partir de una revisión documental que establece el estado de la cuestión, describe la forma en la que incide la IA en el derecho a la privacidad especialmente en el de protección de datos personales, identifica los desafíos normativos en esta materia y posibles soluciones que involucran a los actores que intervienen en los sistemas de inteligencia artificial, particularmente los Estados.

PALABRAS CLAVE

Inteligencia artificial, regulación, derechos humanos, derecho a la privacidad, derecho de protección de datos personales.

ABSTRACT

The objective of the document is the analysis of artificial intelligence from data protection right perspective to identify the challenges for the safeguarding of this human right. The contribution is developed from a documentary review that establishes the actual context, describes how artificial intelligence could affect the right to privacy, especially data protection right and identifies the regulatory challenges in this matter and possible solutions that involve artificial intelligence actors, particularly States.

KEYWORDS

Artificial intelligence, regulation, human rights, right to privacy, data protection right.

---

*Artículo de Investigación postulado el 30 de abril de 2020 y aceptado el 10 de noviembre de 2020

**Profesora investigadora en la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas, México. (andrea.mendoza@cide.edu) orcid.org/0000-0002-4704-740X

SUMARIO

1. Introducción

El vertiginoso desarrollo tecnológico ha permitido que las organizaciones utilicen cada vez más técnicas como la inteligencia artificial, a fin de hacer más eficientes los procesos y la toma de decisiones.

Los usos de la IA son tan variados que pueden ser incorporados en sectores desde la agricultura hasta medios de transporte, por lo que tienen una incidencia en todos los espacios de la sociedad.

Los usuarios digitales también encuentran en la IA una oportunidad para el procesamiento de información, por ejemplo, relativa a su estado de salud, preferencias comerciales, o simplemente para buscar información en el ciberespacio.

Estos beneficios son posibles a partir del análisis masivo y sistemático de la información, que incluye casi siempre, datos personales que identifican o hacen identificables a los humanos.[1]

Derivado de lo anterior, existe una constante preocupación respecto del uso masivo de sistemas de IA que para su funcionamiento requieran de información que identifique o haga identificable a la persona detrás del dato. Esto frente a prácticas como los tratamientos indebidos de datos (falta de cumplimiento normativo o de incorporación de límites éticos), la falta de medidas de seguridad o errores en el diseño de la técnica, que podrían traer consigo la violación de derechos humanos: desde el derecho a la vida, el derecho a la no

[1] No debemos perder de vista que algunos países funcionan como periféricos y que simplemente son consumidores tecnológicos de lo que para algunos países desarrollados resulta obsoleto. La obsolescencia tecnológica que no es casualidad, es un fenómeno propiciado por las corporaciones a partir de la situación de desventaja de países que no tiene desarrolladas sus propias capacidades tecnológicas. Un ejemplo claro, es la compra de pruebas rápidas que detectan el Covid-19 por parte de países como España, que ya han sido descartadas para diagnósticos oportunos y certeros en países como Alemania. La obsolescencia tecnológica también tiene un impacto en la forma en la que los países utilizan y explotan la información y los beneficios que de ello obtienen en la economía digital.

discriminación, el derecho a la salud, hasta el derecho a la privacidad y a la protección de datos personales, por enunciar algunos.

Por otro lado, cuando estamos ante tratamientos de información que contienen datos personales a través de sistemas de inteligencia artificial, ya existe un marco normativo transversal de índole local y en algunos casos regional o internacional, sobre todo en materia de protección de datos personales, por lo que la hipótesis central de este documento es que el desafío del derecho de protección de los datos personales en la IA no es del todo normativo (como podría pensarse), sino de mecanismos que permitan el efectivo ejercicio y garantía de los derechos humanos por parte de los actores involucrados en la IA (desarrolladores, corporaciones y usuarios).

También resulta pertinente analizar si el marco legal de los derechos humanos, en específico el de protección de datos personales permite proteger a la persona frente a técnicas como la inteligencia artificial, a fin de lograr un correcto balance entre innovación y dignidad de la persona.

El lector encontrará en las siguientes líneas una aproximación conceptual de la IA y algunos de sus usos en la economía digital, la forma en la que el derecho de protección de datos personales se ha configurado como un derecho humano, un estudio sobre el derecho a la privacidad y el de protección de datos personales en la IA y un apartado de conclusiones.

2. Concepto de inteligencia artificial y usos en la economía digital

Como ha quedado establecido, el término "inteligencia artificial" aparece desde los años 50 en algunas investigaciones de ciencias de la computación. El concepto fue utilizado por primera vez en 1955 en el proyecto de investigación de John McCarthy, Marvin L. Minsky, Nathaniel Rochester, y Claude Shannon.[2]

También el término de IA en la dimensión atribuida por la informática ha sido explorado por la ciencia jurídica desde 1960. Los primeros documentos jurídicos que hablan de inteligencia artificial lo hacen para referirse a la transcripción de medios de prueba en una forma legible por computadoras para obtener un procesamiento eficiente de la información,[3] así como para procesar la información proporcionada por un cliente a un abogado y determinar la

[2] Mc Carthy, J., *et al*. "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence". AI Magazine. 1955, vol. 27, núm. 4, p. 2. Disponible en: https://doi.org/10.1609/aimag.v27i4.1904.

[3] Gibbs, M., y Adams, (1962). "A report on the second national law and electronics conference". En: MULL: Modern Uses of Logic in Law, [en línea]. V. 3, no. 4, pp. 215–223 [consulta 20-03-20]. Disponible en: www.jstor.org/stable/29760908

probabilidad de ganar un caso, la cantidad estimada de daños si los hubiere, el análisis de la legislación legal, así como la jurisprudencia.[4]

En recientes fechas, el Grupo de Alto Nivel en IA creado por la Comisión Europea para desarrollar la Estrategia Europea en Inteligencia Artificial, ha aplicado el concepto de IA a "sistemas que manifiestan un comportamiento inteligente, al ser capaces de analizar el entorno y realizar acciones, con cierto grado de autonomía, con el fin de alcanzar objetivos específicos".[5]

Desde una perspectiva técnica, entonces podemos afirmar que el término IA se usa en general para referir la capacidad de una máquina para imitar las funciones cognitivas de los humanos; sin embargo, nos encontramos también frente nuevas ramas que derivan del concepto de inteligencia artificial, tales como el aprendizaje de las máquinas (*machine learning*), en el cual, los sistemas aprenden a partir de ejemplos, pruebas o de la información y comportamiento de usuarios de dicho sistema, y los modelos de redes neuronales,[6] por lo que el alcance del concepto de IA irá evolucionado a la par de los avances tecnológicos en la materia.

Una vez que hemos dado una aproximación conceptual a la inteligencia artificial, resulta necesario hablar de algunos de sus usos en la economía digital para identificar las intersecciones específicas con el derecho de protección de datos personales.

De acuerdo al Libro Blanco sobre la IA-un enfoque europeo orientado a la excelencia y la confianza-, el impacto derivado de los usos de los sistemas de IA debe considerarse no solo desde una perspectiva individual, sino también desde la perspectiva de la sociedad en su conjunto y que el uso de sistemas de IA puede tener un papel importante en la consecución de los Objetivos de Desarrollo Sostenible y en el respaldo de los procesos democráticos y los derechos sociales.[7]

Esto resulta importante porque el uso de sistemas de IA no solo beneficia a la persona en lo individual, sino que tiene un impacto social, en los derechos humanos e incluso en las democracias. Es por esta razón que algunos países

[4] Winston, J. (1967). "The Law and Legal Education in the Computer Age." En: Journal of Legal Education, [en línea]. V. 20, no. 2, pp. 159-168. [consulta 12-02-20] Disponible en: www.jstor.org/stable/42891839

[5] Artificial Intelligence for Europe. Comisión Europea, 2018 [consulta 13-03-20]. Disponible en: https://ec.europa.eu/digital-single-market/en/artificial-intelligence

[6] Inteligencia Artificial. Foro Consultivo de Ciencia y Tecnología, 2018 [consulta 13-03-20]. Disponible en: https://www.foroconsultivo.org.mx/INCyTU/documentos/Completa/INCYTU_18-012.pdf.

[7] Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza. Comisión Europea, 2020 [consulta 13-03-20]. Disponible en: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

desarrollados ya han advertido el impacto favorable que tendría la incorporación de sistemas de inteligencia artificial, por lo que han dedicado planes y política pública para el desarrollo de dicha innovación.

Para tener una idea del alcance que se tiene proyectado para la inteligencia artificial, globalmente, Europa se sitúa a la zaga en inversiones privadas en IA, las cuales oscilaron entre 2 400 y 3 200 millones EUR en 2016, frente a 6 500-9 700 millones EUR en Asia y 12 100-18 600 millones EUR en América del Norte.[8]

En el mismo sentido, resulta necesario analizar que el tráfico mundial a través del Protocolo de Internet (IP) pasó de unos 100 gigabytes (GB) al día en 1992, a más de 45.000 GB por segundo en 2017, debiendo considerarse que el mundo solo se encuentra en los principios de la economía basada en datos y que las predicciones son que para 2022 el tráfico IP mundial alcance los 150.700 GB por segundo, alimentado por un número cada vez mayor de personas que se conectan por primera vez y por la expansión de Internet de las Cosas (que funciona con sistemas de inteligencia artificial).[9]

El tipo de IA que ha disparado la aplicación práctica de esta disciplina es la que se conoce como IA-débil[10] que se caracteriza por desarrollar soluciones capaces de resolver un problema concreto y acotado. La aplicación de este tipo de sistemas es extensa: desde los videojuegos a sistemas de defensa, pasando por entorno sanitario, control industrial, robótica, buscadores de Internet, tratamiento de lenguaje natural, marketing, asistentes personales, recursos humanos, optimización de servicios públicos, gestión energética, medioambiente y cualquier otra actividad que nos podamos imaginar.[11]

Por citar algunos ejemplos, en Dinamarca, la IA ayuda a salvar vidas al permitir a los servicios de emergencias diagnosticar paradas cardíacas u otras dolencias analizando la voz de la persona que llama. En Austria, ayuda a los radiólogos a detectar tumores con mayor precisión, al facilitarles la comparación instantánea de las radiografías con una gran cantidad de otros datos médicos.

[8] Op. Cit., nota 5.

[9] Informe sobre la economía digital 2019. Creación y captura de valor: repercusiones para los países en desarrollo. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, UNCTAD. [consulta 30-03-20]. Disponible en: https://unctad.org/es/PublicationsLibrary/der2019_overview_es.pdf

[10] En función del alcance y el ámbito de aplicación de la inteligencia artificial se diferencian tres categorías distintas de IA: las inteligencias artificiales fuertes, generales y débiles. La IA general podría resolver cualquier tarea intelectual resoluble por un ser humano; la IA fuerte o superinteligencia iría más allá de las capacidades humanas.

[11] Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. Agencia Española de Protección de Datos Personales, 2020 [consulta 13-03-20]. Disponible en: 5https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

Muchas explotaciones agrarias de toda Europa ya están utilizando la IA para controlar los desplazamientos, la temperatura y el consumo de los animales. La IA también está contribuyendo a que el sector industrial europeo resulte más eficiente y a que la fabricación vuelva a Europa.[12]

Es fácil entonces, identificar los enormes beneficios que traen consigo los sistemas de inteligencia artificial, pero no se puede obviar una constante preocupación específicamente cuando el insumo de la IA que es la información, contiene datos personales, ya que al ser sistemas que se incorporan en la vida diaria y que recopilan todo tipo de información, pueden tener un impacto considerable a ámbitos privados de las personas, por lo que resulta necesario establecer los límites para el tratamiento de la información y en general, salvaguardar la vida privada de las personas, aún con la utilización de sistemas de inteligencia artificial, por lo que en el apartado cinco, analizaremos algunas de las disposiciones normativas que establecen reglas para el tratamiento de datos en sistemas de inteligencia artificial.

3. Configuración del derecho de protección de datos personales como un derecho humano y sus implicaciones en la inteligencia artificial

Cuando se habla del derecho de protección de datos personales es usual pensar que es un derecho nuevo que nace a partir de la economía digital, del uso de Internet y del vertiginoso desarrollo de las Tecnologías de la Información y Comunicación.

No obstante, si bien es un derecho de reciente reconocimiento en la Constitución Política de los Estados Unidos Mexicanos (2009), tiene antecedentes importantes en la época de posguerra en Europa.

Pensemos así en una Alemania nazi que trató los datos de miles de judíos a través de un censo realizado por el Estado, con la ayuda de las tarjetas perforadas de la empresa IMB, con el objetivo de identificar a esta población y planear su exterminio de forma más efectiva.[13]

[12] Disruptive technologies: Advances that will transform life, business, and the global economy, McKinsey Global Institute, 2013. [consulta 13-03-20]. Disponible en: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/disruptive-technologies

[13] BLACK, Edwin. IBM y el Holocausto. La alianza estratégica entre la Alemania Nazi y la más poderosa corporación norteamericana, Buenos Aires: Atlántida, 2001, p. 18.

A partir de atrocidades como éstas, se volvió evidente la necesidad de establecer límites del Estado frente a la vida privada de las personas y ejemplo de ello está manifestado en el artículo 12 de la Declaración Universal de Derechos Humanos, -en adelante DUDH-.

Antes de analizar este artículo, es pertinente dar un contexto sobre la necesidad histórica de reconocer en instrumentos internacionales un concepto tan importante como la dignidad humana, que hasta el día de hoy, es sustento de los instrumentos jurídicos en materia de derechos humanos. Es decir, a partir de las atrocidades cometidas durante la Segunda Guerra Mundial, países ganadores y vencidos encontraron esencial reconocer derechos mínimos a las personas, en una invocación inédita a la dignidad humana.

Es así, que la manifestación del límite del Estado respecto de la vida privada de las personas está plasmado en el citado artículo 12 de la DUDH, el cual señala:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Como se puede advertir, este artículo no reconoce de forma expresa el derecho de protección de datos personales, pero sí es un antecedente importante para la evolución normativa manifestada a través de nuevos derechos como el de protección de datos personales.

Aunado a la DUDH, existen otros instrumentos internacionales en materia de derechos humanos que reconocen límites del Estado frente a la vida privada de las personas, como el artículo 11 de la Convención Americana de Derechos Humanos[14] (Pacto de San José de Costa Rica), de 1966, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos[15] de 19 de diciembre del mismo año 1966, el artículo 8 del Convenio Europeo de Derechos Humanos[16] de 4 de

[14] "Artículo 11. Protección de la Honra y de la Dignidad 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

[15] "Artículo 17. 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la Ley contra esas injerencias o esos ataques".

[16] "Artículo 8. Derecho al respeto a la vida privada y familiar. 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta

noviembre de 1950 son ejemplo de ello; asimismo, la Carta de los Derechos Fundamentales de la Unión Europea suscrita en Niza el 7 de diciembre de 2000.

Desde el derecho continental, un paso importante para el derecho de protección de datos personales se reconoce cuando el Tribunal Constitucional Federal Alemán, en la sentencia de 15 de diciembre de 1983 sobre el Censo, completó los derechos constitucionales de la personalidad, sobre la base del derecho a la dignidad humana y al libre desarrollo de la personalidad, lo cual garantizó la continuidad de las libertades básicas reconocidas anteriormente, a través de la formulación de un nuevo derecho denominado autodeterminación informativa. Este derecho reconoce la facultad de las personas para decidir sobre el tratamiento de sus datos personales y así garantizar derechos conexos como el derecho a la no discriminación y al libre desarrollo de la personalidad.[17]

En este sentido, el reconocimiento de la dignidad humana resulta el sustento del derecho al libre desarrollo de la persona que es la esencia y fundamento del derecho a la identidad, el de imagen y el de datos personales, a fin de no instrumentalizar a la persona humana. Esto en concordancia con la fórmula del objeto de Kant (*objekt formel*)[18] y su aplicación a este caso: la persona es el fin más no el instrumento (la persona no puede ser tratada como el medio porque no es un objeto en el mercado con un valor determinado). En otras palabras, la IA tendría que ser desarrollada para mejor la vida de los humanos y no para utilizarlos, por ejemplo, a través de tratamientos de datos personales que vulneren derechos como la no discriminación, la privacidad, la protección de datos personales o incluso el derecho a la vida.

Determinar el alcance del derecho humano a la protección de datos personales no es tarea sencilla ya que, al tratarse de un derecho humano, es susceptible de colisionar con otros derechos, por ejemplo, el de la libertad de expresión, por lo que la ponderación de derechos de forma casuística permite a los tribunales establecer los parámetros del derecho de protección de datos personales en el marco de una sociedad democrática.

injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

[17] Sentencia de 15 de diciembre de 1983 emitida por el Tribunal Constitucional Federal Alemán. [consulta 13-03-20]. Disponible en: http://www.informatica-juridica.com/jurisprudencia/alemania.asp.

El principio de consentimiento se analiza en esta Sentencia, anulando la Ley del Censo de Población de 1.982 y dio lugar a una revisión sustancial de la ley federal de 1977, así como las leyes del Ejército y del Servicio Secreto.

[18] Lefranc, Federico, "La necesidad de reafirmar el principio de la dignidad humana en el Derecho del siglo XXI". México Revista Penal México. 2011, no. 2, p. 155, [consulta 13-03-20]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6158028.

El reconocimiento que ha hecho México del derecho de protección de datos personales como un derecho humano tiene interesantes consecuencias ya que derivado de la reforma constitucional en materia de derechos humanos de 2011, el estado mexicano se ve comprometido a salvaguardar y promover este derecho e incluso, la aplicación de principios como el de progresividad de los derechos humanos, compromete a México a evolucionar normativamente en favor de este derecho.

No obstante lo anterior, para el estado mexicano la salvaguarda del derecho de protección de datos personales en el ámbito tecnológico resulta bastante compleja. Esto atendiendo a que se ha depositado una enorme responsabilidad en las corporaciones para que sean éstas las que decidan los términos y condiciones en los que garantizarán los derechos humanos. Es decir, espacios ubicuos como Internet o un sistema de inteligencia artificial, hacen inminente la reducción de la figura tradicional de Estado-Nación, cuando se trata de garantizar y promover los derechos humanos, ya que estas acciones quedan mayormente en manos de las corporaciones.

Pensemos, por ejemplo, si las políticas de privacidad de una cuenta o perfil en una red social están redactadas en términos de la máxima protección que reconoce la norma mexicana para el tratamiento de datos personales, particularmente en términos del ejercicio del derecho de cancelación u oposición para el tratamiento de datos personales, o de la jurisdicción que reconoce la red social para resolver posibles disputas.

Ante este panorama, cada vez se vuelve más necesario incorporar el principio de escrutinio de los derechos humanos como habilitador para el Estado de un mecanismo efectivo para la supervisión, garantía y ejercicio de los derechos humanos a la luz del desarrollo tecnológico.

En este sentido, un caso interesante sobre desarrollo de instrumentos de control estatal que permite la salvaguarda de los derechos humanos en la inteligencia artificial, es el Consejo de la Unión Europea que presentó en febrero de 2019 unas conclusiones relativas al Plan Coordinado sobre la IA "*Made in Europe*", entre las que destaca la importancia de garantizar el pleno respeto de los derechos de los ciudadanos mediante la aplicación de directrices éticas para el desarrollo y uso de la inteligencia artificial.[19]

[19] López, Baroni, (2019). "Las narrativas de la inteligencia artificial. Revista". En: Bioética y Derecho, No. 46, p. 13 [consulta 10-10-20]. Disponible en: https://revistes.ub.edu/index.php/RBD/article/view/27280

Dicho esto, podemos afirmar que, en la mayoría de las legislaciones, se reconoce un catálogo de derechos humanos que pueden verse afectados con la instrumentación de la IA sin límites éticos, jurídicos y sociales

Desde del derecho público, particularmente para el caso de México, también podemos plantear la siguiente interrogante: ¿los Estados deben impulsar e incidir en la transparencia en el desarrollo de algoritmos y sistemas de funcionamiento general de la inteligencia artificial? El planteamiento con miras a hacer posible que la autoridad tenga claros los temas de vigilancia y cumplimiento que deben seguir las corporaciones, respecto de la explotación de la información.

Ante tal panorama, el derecho humano de protección de datos personales tiene retos complejos que superar frente la inteligencia artificial, los cuales radican primordialmente en recuperar la parte humanística relacionada al mismo, para así otorgar certidumbre, generar confianza y ofrecer un entorno digital ético a los usuarios. Reforzando esta idea, es necesario invocar la Declaración de Principios de la Cumbre Mundial sobre la Sociedad de la Información, en la que se estableció el compromiso de construir una sociedad basada en la persona, en la que todos pudiéramos crear, consultar, utilizar y compartir la información y el conocimiento, para impulsar el desarrollo sostenible y mejorar la calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos.[20]

Derivado de lo anterior, podemos afirmar que la idea de dignidad humana debe estar más presente que nunca en el desarrollo tecnológico y en la forma en la que se configura la regulación en torno a dicho rubro, y uno de los grandes desafíos de no hacerlo, es la paradoja de la coordinación y fragmentación de procesos desiguales de desarrollo.[21] Es decir, el desarrollo tecnológico debe preservar un equilibrio entre la libertad y la dignidad humana, el cual podría lograrse a través de un humanismo sólido y del respeto de dicha dignidad como eje de cualquier avance científico: la tecnología como herramienta para empoderar a las personas, pero no como el único fin.

[20] Adelantando un poco la respuesta respecto a los principios ahí establecidos y el resultado de la sociedad digital construida, podemos mencionar el informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos de 2014, denominado el Derecho a la Privacidad en la Era Digital, que deja en relieve la responsabilidad que hasta ahora han tenido las empresas para vulnerar la privacidad de las personas en el ciberespacio. [consulta 13-03-20]. Disponible en: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-In-digital-Age-Spanish-version.pdf

[21] Giddens, A., Consecuencias de la Modernidad, Madrid: Alianza, 1993, p. 162.

Apuntalando lo anterior, el derecho en nuestro siglo tiene el reto de recuperar el carácter humanístico frente al desarrollo tecnológico.[22]

4. Inteligencia artificial y derecho a la privacidad

En este apartado, primero es necesario dar una aproximación a lo que referimos cuando decimos palabras aparentemente iguales, pero que tienen pequeñas variaciones en su significado, necesarias de distinguir cuando queremos preservar la privacidad en tiempos de inteligencia artificial.

Es así que el significado de términos como privacidad, vida privada, y protección de datos personales, tiene alcances distintos.

Iniciando desde la conceptualización del derecho a la privacidad, éste tiene su origen en la doctrina estadounidense de finales del siglo XIX,[23] cuando Warren y Brandeis publicaron su ensayo *The Right to Privacy*, el cual manifestaba el necesario reconocimiento del derecho a no ser molestados (*right to be alone*), y posteriormente Westin amplió este concepto e incluyó dentro del derecho a la privacidad, el derecho de todo individuo para determinar cómo, cuándo y hasta qué punto su información personal es comunicada a los demás.[24]

El fin último que se busca preservar frente a posibles injerencias arbitrarias en la vida privada de las personas, es contar con mecanismos legales que en su conjunto salvaguarden la vida privada. Uno de estos mecanismos, es el derecho de protección de datos personales (que únicamente protege el poder del titular de un dato personal para decidir sobre su tratamiento, salvo excepciones), pero al menos para el caso de México, hay otros instrumentos como el reconocimiento constitucional del secreto de las comunicaciones, la incorporación de figuras del derecho civil que protegen el derecho al honor, a la propia imagen y disposiciones de índole penal que establecen las reglas de geolocalización en tiempo real. Es decir, todas estas disposiciones en su conjunto permiten (en el deber ser), al Estado garantizar la vida privada de las personas.

El concepto "privacidad" no es un concepto terminado y depende del contexto y circunstancias de los casos particulares, poder acotarlo. Es decir, lo que en un país puede considerarse como una situación del ámbito privado, en otro no.[25]

---

[22] Lefranc, F. Terra Incógnita. Bases para una política criminal pro persona en la sociedad digital, México: INFOTEC, 2015, p. 9.

[23] A pesar de que el concepto surge en un sistema de derecho perteneciente al *common law*, esta doctrina ha tenido un impacto provechoso en sistemas jurídicos del derecho continental, como en el caso de México, particularmente para la construcción del derecho a la protección de datos personales.

[24] Westin, A. Privacy and Freedom. Nueva York: Ateneum, 1967, p. 7.

[25] Mendoza, O. Definición de privacidad. En: Diccionario Protección de Datos Personales, INAI, 2020, p. 672. [consul-

En virtud de lo anterior, el término "privacidad" no es fácil de definir, ya que hasta el momento no se tiene una idea clara de sus alcances. Esto se confirma con lo dicho por el Tribunal Europeo de Derechos Humanos, que considera la privacidad como un concepto amplio, no susceptible de una definición exhaustiva.[26]

Para el caso de México, la Suprema Corte de Justicia de la Nación (SCJN) estableció que las afirmaciones contenidas en las resoluciones nacionales e internacionales relacionadas a la privacidad o vida privada son útiles en la medida en que no se tomen de manera descontextualizada, emerjan de un análisis cuidadoso de los diferentes escenarios jurídicos en los que la idea de privacidad entra en juego y no se pretenda derivar de ellas un concepto mecánico de vida privada, de referentes fijos e inmutables. Lo único que estas resoluciones permiten reconstruir, en términos abstractos, es la imagen general que evoca la idea de privacidad en nuestro contexto cultural.[27]

Es así que en términos generales podemos decir que la privacidad es el ámbito más íntimo o profundo de la vida de una persona, que puede comprender sus sentimientos, pensamientos, emociones, vida familiar o relaciones personales y el derecho a la privacidad, el poder que tiene la persona frente a cualquier intromisión de un tercero que pudiera manifestarse (incluido el propio Estado). El derecho a la privacidad es el poder de decisión de una persona sobre su espacio privado, con quién lo comparte, qué debe formar parte de lo público y qué de lo privado.[28]

La privacidad y derecho a la privacidad no necesariamente refieren a lo mismo: la privacidad es un elemento consustancial a la dignidad humana y por ende debe ser protegido por el derecho y el derecho a la privacidad es aquél que todo individuo tiene a separar aspectos de su vida privada del escrutinio público.[29]

---

ta 13-03-20]. Disponible en: http://inicio.inai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf

[26] Piñar, J. "¿Existe privacidad?, Lección magistral impartida en la Apertura Solemne del Curso Académico en la Universidad San Pablo-CEU de Madrid". En: *Protección de Datos Personales. Compendio de lecturas y legislación*. México, 2010, Editorial Tiro Corto, p. 16.

[27] 165823. 1a. CCXIV/2009. Primera Sala. Novena época. Semanario Judicial de la Federación y su Gaceta. Tomo XXX, diciembre de 2009, p. 277. Derecho a la Vida Privada. Su contenido general y la importancia de no descontextualizar las referencias a la misma. [consulta 10-03-20]. Disponible en: http://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/165/165823.pdf. Fecha de consulta: 20 de agosto de 2018.

[28] El derecho a la privacidad no es un derecho absoluto y estará limitado a apreciaciones establecidas en precedentes judiciales como el grado de exposición pública de una persona, la trascendencia en las actividades que realiza, los alcances de protección de la libertad de expresión, el interés público, etc.

[29] Ricci, D. Artículo 16 Constitucional. Derecho a la privacidad. En: *Derechos Humanos en la Constitución: comentarios de jurisprudencia constitucional Interamericana II*. [en línea]. México: Instituto de Investigaciones Jurídicas, p.

Por otro lado, los conceptos de privacidad y vida privada se han redefinido a partir del vertiginoso desarrollo tecnológico, el cual hace posible la sobreexposición de ámbitos que hasta hace unas décadas eran meramente del ámbito privado.

Una vez que hemos tratado de definir o al menos dar una aproximación conceptual de la privacidad, vida privada y derecho de privacidad, podríamos estar preguntándonos entonces, ¿por qué es tan importante preservar la privacidad en tiempos de inteligencia artificial?:

Una primera respuesta es que el valor de la privacidad tiene un componente privado, pero también es un *social good*, en la medida en la que es necesaria para la pervivencia de la democracia y la libertad.[30] Por ejemplo, no podríamos imaginar un estado constitucional y democrático de derecho, frente a censos que utilicen la IA para procesar información de la población, que deriven en un exterminio masivo de personas, como sucedió en la Alemania nazi durante el Holocausto.

Una segunda respuesta sobre la importancia de preservar la privacidad en tiempos de IA tiene que ver con la enorme capacidad técnica de las organizaciones para recabar grandes cúmulos de información en tiempo real, procesarla y tomar decisiones, lo cual expone aspectos privados de la vida de las personas, como los hábitos de consumo de un hogar, los ingresos económicos de una persona o su ideología política o religiosa, por mencionar algunos. Esta sobreexposición y concentración de información por parte de unos cuantos, deja a los usuarios de sistemas de inteligencia artificial, particularmente desprotegidos frente al poder acumulado por las corporaciones y ejemplos como el de *Cambridge Analytical,*[31] hacen evidente la necesidad de vigilar el comportamiento de tecnologías como la inteligencia artificial.

La tercera respuesta está relacionada con el párrafo anterior, ya que el rol de las corporaciones como actores que ostentan el poder en la economía digital propicia la eventual disminución del Estado Nación y la no intervención a

1045. [consulta 2-03-20]. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf.

[30] Contreras, Carlos. *El papel del gobierno en la era digital: un enfoque de economía pública.* 2017, Editorial Universitaria Ramón Arces, p.p. 153 y 154.

[31] Este caso consistió en que la empresa *Cambridge Analytical* tuvo acceso a los datos de unos 87 millones de usuarios de Facebook, según reveló la red social. La información fue obtenida a través de una aplicación que ofrecía realizar un test de personalidad pero que, en realidad usó ese acceso para recopilar datos de los usuarios y de sus redes de amigos hasta sumar hasta un 15% de la población de Estados Unidos. La empresa utilizó este material para elaborar perfiles psicológicos de cada usuario y diseñar mensajes hechos a medida para tratar de influir en las elecciones presidenciales de Estados Unidos de 2016. [consulta 12-03-20]. Disponible en: https://www.bbc.com/mundo/noticias-43971491

través de su rectoría, para la salvaguarda de derechos humanos como el derecho a la privacidad.

Como podemos advertir de las líneas anteriores, el rápido desarrollo tecnológico hace que cada vez sea más complejo garantizar el derecho a la privacidad, ya que la información que se genera a partir del uso de Internet y de sistemas de inteligencia artificial, se encuentra susceptible a ser sometida a tratamientos masivos, y muchas veces sin contar con el conocimiento y consentimiento informado del titular del dato. En este punto, es conveniente resaltar que hoy día, la IA permite en algunos casos hacer tratamiento de datos legales pero poco éticos, ya que si bien los sistemas son programados para cumplir en el mejor de los casos, con los requisitos mínimos de las normas, (en materia de protección de datos personales sería el consentimiento de los titulares de la información), este consentimiento no es verdaderamente informado, o no se propician los mecanismos necesarios para que los titulares de datos alcancen a entender la dimensión de la autorización.[32]

5. El derecho de protección de datos personales en los sistemas de inteligencia artificial

Como hemos visto en apartados previos, el artículo 12 de la Declaración Universal de Derechos Humanos, reconoce el derecho a la no injerencia en la vida privada de las personas, el cual puede considerarse el antecedente más importante, que estableció las bases para una evolución normativa e incorporación a los marcos legales domésticos de distintas figuras jurídicas, que en su conjunto protegen la vida privada de las personas.

Una de estas figuras, es el derecho de protección de datos personales, el cual fue reconocido en 2009, en la Constitución Política de los Estados Unidos Mexicanos, mediante adhesión de un párrafo al artículo 16, el cual, señala:

"Artículo 16. ...

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar

[32] En este punto, es fácil escuchar discursos que criminalizan a los usuarios de sistemas de inteligencia artificial, por otorgar el consentimiento sin comprender las dimensiones del tratamiento de la información, pero se debe tener en cuenta, primero la falta de educación digital de los usuarios (porque existe muy poca política pública efectiva de educación e inclusión digital en México), en segundo lugar, los condicionamientos para la prestación de servicios necesarios, incluso aunque sean contrarios a las normas nacionales, tercero, la instrumentación de cláusulas de adhesión en los contratos y cuarto, la responsabilidad final y única de las corporaciones para insertar aspectos éticos en el tratamiento de datos, que pudieran generar confianza.

> su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.
>
> ...".[33]

El derecho de protección de datos personales le confiere al titular del dato, el poder de decisión sobre el tratamiento de su información, desde que se recaba hasta que se destruye. Este derecho cobra vida a través de los denominados derechos ARCO, también reconocidos en el referido artículo 16 de la carta magna, y consistentes en los derechos de: acceso, rectificación, cancelación y oposición frente al tratamiento de datos personales.[34]

No obstante, como pasa con otros derechos humanos, el de protección de datos personales no es un derecho absoluto y encuentra sus restricciones en el multicitado artículo 16 constitucional, al referir que todas las personas gozarán del derecho de protección de datos personales, salvo que exista un impedimento o restricción por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger derechos de terceros.

En otras palabras, el derecho de protección de datos personales encuentra sus límites en aquellas excepciones reconocidas expresamente en el 16 constitucional y que resultan necesarias en sociedad democrática.

El derecho de protección de datos personales en México ha sido regulado en dos normas: La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010) y la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (2017).

En general, estas normas, la primera de índole federal y la segunda de aplicación nacional, reconocen los principios que deben regir el tratamiento de datos personales, las obligaciones de los Responsables y Encargados del tratamiento, las medidas de seguridad que deben considerarse, los procedimientos de denuncia que tiene la persona frente a la vulneración de este derecho y los mecanismos de sanción que tiene el Instituto Nacional de Transparencia,

[33] México. Constitución Política de los Estados Unidos Mexicanos. Diario Oficial de la Federación el 5 de febrero de 1917. P. 17.

[34] A partir de la publicación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (ley de datos cuyo ámbito de aplicación es el sector público), se ha discutido si el reconocimiento en la norma de la portabilidad del dato debe considerarse o no una extensión de los llamados derechos ARCO. En opinión de la autora, la portabilidad no es más que una forma de manifestación del derecho de acceso a los datos personales.

Acceso a la Información y Protección de Datos Personales (INAI) frente al incumplimiento de las disposiciones legales en la materia.

El camino del derecho de protección de datos personales en México desde la perspectiva normativa, parece ser un camino largo y sólido que brinda dos leyes que regulan el tratamiento de datos personales tanto en empresas como en el sector público, e incluso reconoce la coexistencia de algunas normas sectoriales con disposiciones en la materia, que también constituyen excepciones dentro del régimen general de este derecho, como la Ley de Instituciones de Crédito.

No obstante, cuando hablamos del derecho de protección de datos personales en ámbitos digitales o tecnológicos, como lo es el de la inteligencia artificial, -por las características propias de las innovaciones-, parece que el alcance de este derecho se diluye respecto de los alcances efectivos que sí tiene en el mundo físico.

El efectivo ejercicio de derechos ARCO en sistemas de IA a veces resulta casi imposible, por ejemplo, la dificultad de ejercer los derechos de acceso y/o rectificación previa a una posible vulneración de derechos humanos frente al tratamiento de datos personales que haga un sistema de identificación facial utilizado por el Estado. Es decir, el sistema de IA funcionará con la información que haya suministrado alguna entidad estatal, haciendo casi imposible el acceso, la rectificación o cancelación del dato, antes o después de una vulneración a un derecho humano como podría ser el de libertad de expresión.

Aunado a esto, pensemos en la falta de transparencia en el funcionamiento de estos sistemas de identificación facial, ya que muchos de ellos trabajan con información de la población en general y no solo de aquellos individuos que representan por cualquier motivo válido en una sociedad democrática, un riesgo para la seguridad pública o la seguridad nacional y en la medida desproporcionada en la que los sistemas de identificación son utilizados por parte de los Estados.

Tal vez en este ejemplo, el sistema de IA de identificación facial constituya por sí mismo una vulneración a la libertad de expresión en una sociedad democrática, que establece una medida sistemática y previa de censura y desproporcionada por parte del Estado. Esta conclusión que nada aparentemente tiene que ver con el derecho de protección de datos personales, se pude elaborar a partir del análisis del tipo de datos que trata un sistema, los fines para llevar a cabo dicho tratamiento y una evaluación a la luz del principio de proporcionalidad en materia de datos personales.

Lo anterior, sin tomar en consideración que la IA permite incorporar nuevas posibilidades que representan desafíos para los derechos humanos, por

ejemplo, el análisis de emociones a través de lo que una persona publica en una red social y un algoritmo que calcule el riesgo que su estado anímico, pensamientos, ideología, representa para la seguridad de un Estado.

En este ejemplo, las políticas de privacidad de las redes sociales desempeñan un papel importante, por ejemplo, los usuarios que fueron analizados para crear perfiles psicológicos por la empresa *Cambridge Analytical*, lo hicieron proporcionando su consentimiento para el tratamiento de datos en general, y dicha autorización la hicieron cuando fueron condicionados a otorgarla para usar una aplicación de proyección del futuro.

Este último punto permite la reflexión sobre el enorme peso que desde el modelo mexicano de regulación en materia de datos personales se ha depositado sobre el principio de información y su manifestación través del aviso de privacidad, ya que el cumplimiento tanto del principio de información como el de consentimiento a través de dicho aviso, no asegura un tratamiento ético de la información. Es decir, estamos frente a tratamientos lícitos de datos personales, pero no éticos.

Es pertinente matizar el ejemplo diciendo que el enorme desafío que se advierte respecto del derecho de protección de datos personales en la IA es el de lograr un balance que permita aprovechar los beneficios de esta tecnología, sin poner en peligro la dignidad de las personas y sus derechos fundamentales. Esto no parece sencillo, por lo que elementos como la transparencia, el escrutinio de la proporcionalidad en el uso de sistemas de inteligencia artificial, la incorporación de esquemas de cumplimiento normativo y ético, los mecanismos de supervisión estatal y de defensa frente a afectaciones derivadas de decisiones automatizadas, permitirían hacer frente a los peligros que hoy día preocupan a expertos en la materia.

Es decir, en palabras de Federico Lefranc, no hay que equivocarse, la crítica no es a la evolución de la tecnología, ni tampoco frente a sus posibilidades ni frente a sus usos. La crítica se dirige a la concepción epistemológica del discurso, en el entendido de que esta concepción se puede articular entendiendo al sujeto como receptor de dicho discurso.[35]

También el derecho de protección de datos personales en la IA se debe estudiar bajo la óptica del fenómeno de los países periféricos (consumidores de tecnología que no generan o desarrollan sus propias capacidades de ciencia, tecnología e innovación), los cuales casi siempre ven reducido su marco normativo, frente las políticas de privacidad de las corporaciones trasnacionales,

[35] *Op. Cit.*, nota 22, p. 44.

que no son compatibles necesariamente, con la dimensión, que por ejemplo México, le ha dado al derecho humano de protección de datos personales.

Es decir, cuando hablamos de tecnología, a pesar de que México cuenta con un marco legal en materia de protección de datos personales robusto, que retoma los más altos estándares de protección de la persona, en la lógica del modelo de regulación europeo y de la familia romano germánica, todos estos esfuerzos se ven reducidos frente a sistemas de IA que han sido diseñados principalmente en países desarrollados cuya familia jurídica pertenece al derecho anglosajón.

A nivel global existen desarrollos de IA que han despertado el interés y preocupación de muchos Estados, pensando por ejemplo en los sistemas de defensa y en los robots autónomos cuya tendencia en su desarrollo es que puedan tratar datos personales en tiempo real (imágenes) y tomar decisiones sobre los blancos de ataque. Esto considerando si el derecho internacional humanitario alcanza o no para regular los límites que deben tener en cuenta los desarrolladores al momento de programar el *software*. Por ejemplo, la viabilidad de preguntarse si es lícito o no programar un robot para comparar con una base de datos, imágenes de niños y civiles para descartarlos como blanco de ataque y la autonomía de decisión del robot.

Como respuesta a algunas de las preocupaciones generadas a partir de los ejemplos citados, se han creado instancias que trabajan sobre las directrices que debe seguir el desarrollo de IA y cuyo eje transversal sin duda alguna, serán las reglas y límites para el tratamiento de información personal. Un ejemplo interesante de los esfuerzos que supone el uso de la IA protegiendo a la persona frente a tratamientos de sus datos, lo encontramos en el documento de la Agencia Española de Protección de Datos Personales, denominado "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción"[36], en el que se puede encontrar un modelo de incorporación de disposiciones normativas en materia de datos a sistemas de inteligencia artificial.

Retomando el caso de México en los ejemplos mencionados, se puede advertir que si bien el país ha reconocido a nivel constitucional el derecho de protección de datos personales cuenta con normas secundarias que dan vida a este derecho (Ley Federal de Protección de Datos Personales en Posesión de los Particulares de 2010 y Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados de 2017), el nivel de protección de la persona

[36] Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. Agencia Española de Protección de Datos Personales, 2020 [consulta 11-03-20]. Disponible en: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

frente a la tecnología no puede garantizarse cuando hablamos de inteligencia artificial, debido a fenómenos como la ubicuidad, la no existencia de fronteras físicas, la extraterritorialidad de la normas, la reducción del Estado Nación (al depositarse principalmente la garantía de derechos humanos en manos de las corporaciones), la falta de mecanismos estatales de supervisión y garantía de los derechos humanos en la inteligencia artificial.

Es decir, los esfuerzos de los Estados para la salvaguarda de los derechos humanos en ámbitos tecnológicos, especialmente Internet e inteligencia artificial, muchas veces se ven diluidos en la globalización de la era digital.

A pesar de que la falta de mecanismos efectivos para el ejercicio del derecho de protección de datos personales en la IA podría ser el principal problema al que se enfrenta este derecho, no debemos dejar de advertir dos cosas.

Las leyes nacionales en materia de datos personales no contienen disposiciones específicas para el tratamiento de datos personales en sistemas de inteligencia artificial, lo cual no sería un problema determinante, salvo que por las características de dicho tratamiento y la forma en la que funciona la técnica, es necesario cuestionarse sobre la necesidad de configurar nuevos derechos que permitirían la efectiva garantía de la dignidad humana frente a sistemas de inteligencia artificial. Estos derechos son: el "derecho a la no identificación" de las personas en la utilización de inteligencia artificial, el "derecho a que la información personal no sea tratada mediante técnicas de inteligencia artificial" o incluso un "derecho de reclamación" frente a afectaciones a los derechos de las personas, derivadas de las decisiones tomadas mediante sistemas de inteligencia artificial.

Es decir, el marco jurídico de los derechos humanos, en específico el del derecho de protección de datos personales, sirve para establecer las reglas para el tratamiento de datos a través de sistemas de inteligencia artificial, por ejemplo, los principios, deberes, obligaciones y mecanismos para el ejercicio de los derechos ARCO. No obstante, como consecuencia de los tratamientos automatizados de datos personales a través de inteligencia artificial, empieza a hacerse necesario el reconocimiento de nuevas modalidades de ejercicio del derecho de protección de datos personales que incluso servirían para garantizar otros derechos humanos, como el de no discriminación (que no es objeto de este trabajo).

Ahora bien, no se puede hablar del derecho de protección de datos personales en sistemas de IA sin mencionar que al ser la información un valor muy preciado en la economía digital, este derecho tiene también lugar en las negociaciones de tratados internacionales, no sólo de derechos humanos, sino comerciales también.

Es así que cuando hablamos de protección de datos personales e inteligencia artificial, resulta necesario situarnos en la influencia que han tenido instrumentos jurídicos internacionales en la construcción y forma de interpretación de este derecho en México.

En este sentido, en 2018 México fue aceptado al Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, -un instrumento paradigmático en materia de protección de datos personales en el ámbito europeo y de países terceros que sean aceptados a formar parte de éste)-, lo cual establece las bases para una máxima protección de la información de las personas, en un reconocimiento jurídico, histórico y político de la dignidad humana frente al desarrollo tecnológico.

Este paso tan significativo para México ha tenido una etapa de estancamiento, en donde hoy día, existen amenazas directas al reconocimiento que ha hecho el país sobre el derecho de protección de datos personales. Esta afirmación tiene sustento en la aceptación por parte de México de cláusulas contenidas en un instrumento primordialmente económico como el Tratado comercial entre México, Estados Unidos de Norteamérica y Canadá (TMEC), que están por debajo del nivel de protección que el país se comprometió a otorgar en 2018, a través del citado Convenio 108.[37] Otro elemento que apuntala la afirmación de que el derecho de protección de datos personales se ha visto estancado en México, es la falta de voluntad política y legislativa para solicitar la adhesión al Convenio 108 Plus del Consejo de Europa, que permitiría a México terminar la armonización del marco legal doméstico con las normas en el ámbito europeo en materia de protección de datos personales, paso necesario para la consolidación de modelos de comercio digital, cooperación internacional entre autoridades y en general, para la transferencia internacional de datos personales.

Sobre el capítulo 19 de comercio digital del TMEC, el artículo 19.8 habla sobre la protección de la información personal, e inicia haciendo un reconocimiento de los beneficios económicos y sociales de la protección de la información personal de los usuarios del comercio digital y la contribución que dicha protección aporta para generar confianza en el consumidor. En principio, este artículo otorga un margen de apreciación para que cada Estado, adopte o mantenga un marco legal que disponga la protección de la información personal de los usuarios de comercio digital, e incluso señala que cada Estado, podrá tomar

[37] Tratado entre Estados Unidos de Norteamérica, Canadá y México en materia comercial. [consulta 17-03-20]. Disponible en: https://www.gob.mx/t-mec

en consideración los principios y directrices de los organismos internacionales pertinentes, tales como el Marco de Privacidad de APEC y la Recomendación del Consejo de la OCDE relativa a las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales (2013).

Los Estados también reconocen la importancia de asegurar el cumplimiento de las medidas para proteger la información personal y asegurar que las restricciones a los flujos transfronterizos de información personal sean necesarias y proporcionales a los riesgos presentados.[38]

Lo que llama la atención de este capítulo, es el numeral 6 que indica:

"6. Reconociendo que las Partes podrán tomar diferentes enfoques legales para proteger la información personal, cada Parte debería fomentar el desarrollo de mecanismos para promover la compatibilidad entre estos diferentes regímenes. Las Partes procurarán intercambiar información sobre los mecanismos aplicados en sus jurisdicciones y explorarán maneras de extender estos u otros acuerdos adecuados para promover la compatibilidad entre estos. Las Partes reconocen que el sistema de Reglas de Privacidad Transfronterizas de APEC es un mecanismo válido para facilitar las transferencias transfronterizas de información mientras se protege la información personal".[39]

En este sentido, la Comisión Europea ya se ha pronunciado sobre elementos que se deben advertir al momento de negociar tratados internacionales en materia comercial, dejando sentado que los aspectos económicos no pueden estar por encima de los derechos humanos.

También se debe resaltar que si bien la adhesión de México al Convenio 108 del Consejo de Europa, establece un antecedente inédito para indicar el rumbo hacia donde debe evolucionar normativamente este derecho en el marco legal doméstico, (atendiendo primero, al principio de progresividad de los derechos humanos y en segunda lugar, al principio *pro persona* y la interpretación conforme, reconocidos en la Constitución, a partir de la reforma de derechos humanos de 2011), están pendientes los trabajos de adhesión para el citado Convenio 108 Plus, que ya prevé el impacto transversal de la tecnología en la vida privada de las personas.

Esto no es nada menor, ya que países como República Dominicana, hoy día se encuentran analizando y estableciendo las bases para solicitar la adhesión al Convenio 108 plus y México ha tenido retrocesos al aceptar disposiciones

[38] Se recomienda revisar las restricciones señaladas por la Unión Europea a Estados Unidos de Norteamérica y antecedentes como el *Safeharbor*.

[39] Capítulo 19 de Comercio Digital del TMEC. [consulta 17-03-20]. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/465801/19ESPComercioDigital.pdf

de menor protección para el tratamiento de datos personales, previstas en el apartado de comercio electrónico del propio TMEC.

Este fenómeno tiene su explicación en la forma en la que el valor económico de los datos prevalece sobre el reconocimiento del derecho de protección de datos personales del modelo europeo, que considera la dignidad humana como el eje rector para el desarrollo tecnológico, de ciencia y de innovación, y hace un enérgico llamado a las corporaciones a insertar aspectos éticos que sirvan como límites frente a tratamientos que atenten en contra de la dignidad de las personas.

Es decir, en su momento, México decidió sobre el modelo de regulación por el que optaría, siendo el modelo europeo de protección de datos personales el que consideró el más idóneo y dicho modelo, también incluye algunas directrices para la IA y el tratamiento de la información de carácter general, por lo que en el marco del estado constitucional y democrático de derecho, se tendría que guardar congruencia a este reconocimiento y protección de la dignidad de las personas logrando un balance entre los intereses comerciales o económicos que podrían estar contenidos en otros instrumentos internacionales posteriores a la adhesión de México al referido Convenio 108.

Para una mejor explicación del tema, en el caso de la Unión Europea, fue la Comisión Europea la que aprobó las disposiciones para los flujos de datos transfronterizos, derivadas del cierre de la consulta sobre la orientación del artículo 49 del Reglamento Europeo de Protección de Datos Personales. Estas disposiciones se aprueban como horizontales para los flujos de datos transfronterizos y la protección de datos personales en los acuerdos comerciales, ya que los datos personales son un derecho fundamental, que no pueden ser objeto de negociación en los acuerdos comerciales de la UE.

Es decir, la Comisión Europea está tratando de romper las barreras al flujo de datos entre empresas, en futuros acuerdos comerciales como parte de su impulso hacia una economía más digital, al tiempo que salvaguarda los principios fundamentales del derecho de protección de datos personales.

Las disposiciones están diseñadas para insertarse en futuros acuerdos comerciales y garantizar que los principios subyacentes al Reglamento Europeo de Protección de Datos Personales no se vean socavados. Lo interesante de esta propuesta para suscribir acuerdos internacionales por la que optó la Unión Europea, es que las cláusulas relativas a datos personales incluidas en un tratado comercial, serán excluidas de cualquier tribunal de inversión establecido por el

acuerdo para arbitrar y resolver disputas, lo que significa que las disposiciones estarán sujetas a la jurisdicción del tribunal más alto de la Unión Europea.[40]

Derivado de lo anterior, el TMEC si bien reconoce el margen de apreciación para que un Estado regule a través de sus normas domésticas el derecho de protección de datos personales, establece las normas del Foro de Cooperación Económica Asia-Pacífico (APEC), como un punto de encuentro para realizar transferencias internacionales de datos, lo cual no está redactado en términos de lo resuelto por la Comisión Europea, específicamente en el tema de la resolución de controversias, ya que no sería el alto tribunal europeo quien resuelva una posible controversia, sino probablemente los árbitros señalados dentro de los mecanismos alternativos que reconoce el Foro, lo cual propiciaría que si no se cumplen las disposiciones de datos que ya se tienen en México, su revisión no recaería sobre una instancia europea (cuando las transferencias involucren datos de personas nacidas o que vivan en alguno de los países miembros de la Unión Europea), sino en la instancia señalada por el propio APEC. Esto sería algo menor si México no fuera parte del Convenio 108 del Consejo de Europa.

Por otro lado, resaltar que México aún no ha sido declarado país seguro (país tercero fuera de Europa que brinda garantías para un debido tratamiento de datos que reciba por transferencia), por lo que los acuerdos comerciales hacia Europa, podrían verse mermados por esta situación y por la falta de voluntad de alinear las normas locales con los compromisos internacionales, específicamente del ámbito europeo a los que México se comprometió.

En este sentido, los Acuerdos de Puerto Seguro desempeñan un rol importante porque pueden ser los puentes por los que se intercambien datos personales entre uno de los países miembro de la Unión Europea con países que no tienen el mismo nivel normativo de protección del dato, como el caso de Estados Unidos de Norteamérica.[41]

En 2015 el Tribunal de Justicia de la Unión Europea declaró la invalidez del acuerdo sobre la transferencia internacional de datos personales pues entendía

[40] Guidelines on Article 49 of Regulation 2016/679. Consejo de Europa, 2018, [consulta 30-03-20]. Disponible en: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614232

[41] El 16 de julio de 2020 el Tribunal de Justicia de la Unión Europea (TJUE) ha hecho pública una sentencia en la que anula la Decisión 2016/1250 de la Comisión que declaraba el nivel adecuado de protección del esquema del Escudo de Privacidad (*Privacy Shield*) para las transferencias internacionales de datos a EEUU. Esta Decisión sustituía a su vez a Puerto Seguro que también fue declarado inválido por el TJUE en octubre de 2015. La sentencia, cuyas implicaciones marcan un nuevo punto de inflexión sobre la forma en la que se realizan las transferencias internacionales de datos a EEUU, establece, a su vez, la validez de las cláusulas contractuales estándar adoptadas por la Comisión Europea para realizar transferencias internacionales de datos entre un Responsable establecido en la Unión Europea y un Encargado del tratamiento fuera de la UE. [consulta 17-03-20]. Disponible en: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf

que la legislación estadounidense no brindaba las garantías suficientes para proteger aquella información que provenía del espacio europeo.

Tras un nuevo acuerdo, en julio del 2020, el mismo tribunal declaró la invalidez del escudo *privacy shield* como herramienta jurídica válida para garantizar el derecho de protección de los datos de los ciudadanos europeos en supuestos de transferencia internacional.[42]

La figura de los Acuerdos de Puertos Seguro pueden ser una vía idónea para que México transfiera datos personales al país del norte, a fin de tener certeza sobre el tipo de tratamiento proporcional y razonable que haga el país receptor y que el tratamiento de la información no derive en vulneraciones a la dignidad humana, como pasó con los datos personales de migrantes, que instancias mexicanas compartieron con autoridades migratorias de Estados Unidos.

En la región iberoamericana (que privilegia el derecho continental), se han trabajado documentos de *soft law*, que sirven como orientadores para comprender las necesidades regulatorias en el tratamiento de datos en la inteligencia artificial.

El primer documento que analizaremos se denomina "Recomendaciones generales para el tratamiento de datos en la Inteligencia Artificial" de la Red Iberoamericana de Protección de Datos, el cual está dirigido a desarrolladores de productos de IA y da recomendaciones generales, entre las que destacan la elaboración de estudios de impacto de privacidad, la ética y seguridad desde el diseño, *accountability,* esquemas de gobernanza, respeto a los derechos de los titulares del dato, etcétera.[43]

De este documento es importante destacar que no tiene como pretensión oponerse a que las corporaciones traten datos personales a través de la inteligencia artificial, sino que lo hagan con las garantías necesarias, atendiendo las reglas, principios y derechos que dan vida a la protección de datos personales, para así evitar cualquier daño, abuso o vulneración de los derechos de los titulares de esos datos.

La guía se acompaña por un documento más específico, emitido también por la Red Iberoamericana de Protección de Datos Personales, denominado "Orientaciones específicas para el cumplimiento de los principios y derechos

[42] La última Sentencia es la STJUE (Gran Sala) del 16 de julio del 2020. Asunto C-311/18 que tuvo por objeto resolver una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la High Court (Tribunal Superior, Irlanda).

[43] Recomendaciones generales para el tratamiento de datos en la Inteligencia Artificial. Red Iberoamericana de Protección de Datos, 2019, [consulta 18-03-20]. Disponible en: https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf

que rigen la protección de datos personales en los proyectos de inteligencia artificial",[44] en el marco del instrumento normativo que constituye la referencia común para las entidades integrantes de la señalada Red, como son los Estándares de Protección de Datos Personales para los Estados Iberoamericanos que se aprobaron en Santiago de Chile, en 2017.

Otro documento normativo paradigmático en favor del derecho de protección de datos personales vinculado con disposiciones específicas sobre IA es el Reglamento General de Protección de Datos (RGPD) aplicable en el ámbito europeo, el cual refuerza los requisitos relacionados con las decisiones automatizadas, basadas en el uso de inteligencia artificial; es decir, las entidades que utilicen algoritmos (insumos de la inteligencia artificial) tendrán que proporcionar una explicación sobre la lógica de las decisiones automatizadas y sobre sus consecuencias principales para los individuos, pudiendo éstos pedir la intervención humana y recurrir la decisión (principio de transparencia).[45]

Derivado de lo anterior, se advierte que si bien se cuenta con un marco normativo que establece los límites para el tratamiento de datos personales a través de sistemas de inteligencia artificial, resulta necesario pensar en la configuración de mecanismos específicos para que los Estados supervisen el cumplimiento de los alcances de este derecho humano en la IA (principio de escrutinio) y habilitar nuevas manifestaciones del derecho de protección de datos personales para que los titulares tengan mecanismos concretos de defensa frente a las consecuencias de los tratamientos de datos a través de IA (mecanismos de reclamación, de no identificación y de no tratamiento de datos en sistemas de inteligencia artificial).

6. Conclusiones

De las líneas anteriores se ha podido identificar que la IA tiene diversos usos que impactan en todas las esferas de la sociedad. Los beneficios de su incorporación son evidentes por lo que empresas y gobiernos se encuentran explorando nuevas posibilidades de uso y explotación de esta técnica.

[44] Orientaciones específicas para el cumplimiento de los principios y derechos que rigen la protección de datos personales en los proyectos de inteligencia artificial. Red Iberoamericana de Protección de Datos, 2019, [consulta 18-03-20]. Disponible en: https://www.redipd.org/sites/default/files/2020-02/guia-orientaciones-espec%C3%ADficas-proteccion-datos-ia.pdf

[45] Adecuación al Reglamento General de Protección de Datos de tratamientos que incorporen Inteligencia Artificial. Agencia Española de Protección de Datos Personales. [consulta 18-03-20]. Disponible en: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

La IA funciona principalmente a través del procesamiento masivo de información (que puede contener datos personales) lo cual despierta enormes preocupaciones para su instrumentación.

En este sentido, si bien existe un marco legal robusto en materia de datos personales en México, se han identificado algunos de los desafíos para la salvaguarda de este derecho cuando se trata de entornos tecnológicos, específicamente en la inteligencia artificial.

Estos desafíos, relacionados con la extraterritorialidad de la norma, la no existencia de fronteras físicas, las múltiples jurisdicciones interactuando, la reducción del Estado Nación, la responsabilidad otorgada para que sean las corporaciones las que salvaguarden derechos humanos como el de privacidad y datos, diluyen en un mundo digital global el alcance que tiene el derecho de protección de datos en el mundo físico. Esto particularmente desde los países periféricos, que no actúan en bloque regional y que no tienen mecanismos efectivos de obligatoriedad y cumplimiento de sus normas nacionales.

Aunado a lo anterior, se ha identificado la necesidad de reconocer la configuración de nuevas manifestaciones del derecho de protección de datos personales, atendiendo la forma en la que funciona y se incorporan los sistemas de inteligencia artificial, tales como el derecho de reclamación frente a decisiones automatizadas, el derecho a no ser sometido a tratamientos de datos a través de IA y el derecho a que la persona no sea identificada en los tratamientos a través de esta técnica.

Derivado de lo anterior, podemos afirmar que el derecho de protección de datos personales desde su ámbito de derecho humano permite establecer en general las reglas para el tratamiento de los datos personales en la inteligencia artificial, como los principios, los deberes y las obligaciones que Responsables y Encargados deben tener en cuenta. No obstante, la forma en la que se ha diversificado su uso hace necesario hablar de nuevas manifestaciones del derecho de protección de datos personales como las referidas en el párrafo previo, que en su conjunto permitirían incluso proteger otros derechos humanos, como el derecho a la no discriminación.

Por otro lado, frente al crecimiento exponencial de la inteligencia artificial, nos encontramos que los sistemas son programados para cumplir requisitos formales normativos para el tratamiento de datos personales, sin que esto signifique que sean tratamientos éticos; es decir, estamos frente a tratamientos lícitos, pero en muchos casos no éticos.

Desde la óptica de los tratados internacionales, México debe suscribir solo aquéllos que estén armonizados con los compromisos internacionales que el

país ha asumido, relativos a la salvaguarda de los derechos humanos de las personas y su dignidad, particularmente respecto del derecho de protección de datos personales.

Finalmente, México tiene una oportunidad para fungir como país líder hacia una integración regional que estandarice las normas en materia de protección de datos personales aplicadas a la inteligencia artificial, optando por el modelo europeo, que al menos para los países de Iberoamérica, resulta el más compatible, en términos de la herencia del derecho continental y la forma en la que se han configurado los sistemas jurídicos domésticos.

Bibliografía

Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. Agencia Española de Protección de Datos Personales, 2020 [Consulta 13-03-20]. Disponible en: 5https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

Artificial Intelligence for Europe. Comisión Europea, 2018 [consulta 13-03-20]. Disponible en: https://ec.europa.eu/digital-single-market/en/artificial-intelligence

Black, Edwin. IBM y el Holocausto. La alianza estratégica entre la Alemania Nazi y la más poderosa corporación norteamericana, Buenos Aires: Atlántida, 2001, p. 18.

Contreras, Carlos. El papel del gobierno en la era digital: un enfoque de economía pública. 2017, Editorial Universitaria Ramón Arces, pp. 153 y 154.

Disruptive technologies: Advances that will transform life, business, and the global economy, McKinsey Global Institute, 2013. [Consulta 13-03-20]. Disponible en: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/disruptive-technologies

GIBBS, M., y Adams, (1962). "A report on the second national law and electronics conference". En: MULL: Modern Uses of Logic in Law, [en línea]. V. 3, no. 4, pp. 215–223 [consulta 20-03-20]. Disponible en: www.jstor.org/stable/29760908

Giddens, A., Consecuencias de la Modernidad, Madrid: Alianza, 1993, p. 162.

Guidelines on Article 49 of Regulation 2016/679. Consejo de Europa, 2018, [Consulta 30-03-20]. Disponible en: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614232

Informe Anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos denominado el Derecho a la Privacidad en la Era Digital. Disponible en: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-In-digital-Age-Spanish-version.pdf

Informe sobre la economía digital 2019. Creación y captura de valor: repercusiones para los países en desarrollo. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, UNCTAD. [Consulta 30-03-20]. Disponible en: https://unctad.org/es/PublicationsLibrary/der2019_overview_es.pdf

Inteligencia Artificial. Foro Consultivo de Ciencia y Tecnología, 2018 [Consulta 13-03-20]. Disponible en: https://www.foroconsultivo.org.mx/INCyTU/documentos/Completa/INCYTU_18-012.pdf.

Lefranc, Federico, "La necesidad de reafirmar el principio de la dignidad humana en el Derecho del siglo XXI". México Revista Penal México. 2011, no. 2, p. 155, [Consulta 13-03-20]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6158028

Lefranc, F. Terra Incógnita. Bases para una política criminal pro persona en la sociedad digital, México: INFOTEC, 2015, p. 9.

Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza. Comisión Europea, 2020 [consulta 13-03-20]. Disponible en: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf

López, Baroni, (2019). "Las narrativas de la inteligencia artificial. Revista". En: Bioética y Derecho, No. 46, p. 13 [consulta 10-10-20]. Disponible en: https://revistes.ub.edu/index.php/RBD/article/view/27280

Mc Carthy, J., *et al*. "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence". AI Magazine. 1955, vol. 27, núm. 4, p. 2. https://doi.org/10.1609/aimag.v27i4.1904.

Mendoza, O. Definición de privacidad. En: Diccionario Protección de Datos Personales, INAI, 2020, p. 672. [Consulta 13-03-20]. Disponible en: http://inicio.inai.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf

Orientaciones específicas para el cumplimiento de los principios y derechos que rigen la protección de datos personales en los proyectos de inteligencia artificial. Red Iberoamericana de Protección de Datos, 2019, [Consulta 18-03-20]. Disponible en: https://www.redipd.org/sites/default/files/2020-02/guia-orientaciones-espec%C3%ADficas-proteccion-datos-ia.pdf

Piñar, J. "¿Existe privacidad?, Lección magistral impartida en la Apertura Solemne del Curso Académico en la Universidad San Pablo-CEU de Madrid". En: Protección de Datos Personales. Compendio de lecturas y legislación. México, 2010, Editorial Tiro Corto, p. 16.

Recomendaciones generales para el tratamiento de datos en la Inteligencia Artificial. Red Iberoamericana de Protección de Datos, 2019, [consulta 18-03-20]. Disponible en: https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf

Ricci, D. Artículo 16 Constitucional. Derecho a la privacidad. En: Derechos Humanos en la Constitución: comentarios de jurisprudencia constitucional Interamericana II. [En línea]. México: Instituto de Investigaciones Jurídicas, p. 1045. [Consulta 2-03-20]. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf.

Westin, A. Privacy and Freedom. Nueva York: Ateneum, 1967, p. 7.

Winston, J. (1967). "The Law and Legal Education in the Computer Age." En: Journal of *Legal* Education, [en línea]. V. 20, no. 2, pp. 159-168. [Consulta 12-02-20] Disponible en: www.jstor.org/stable/42891839

Sentencias

Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 16 de julio de 2020 Disponible en: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf

Sentencia C311/18 de la STJUE (Gran Sala) de 16 de julio del 2020 del Tribunal Superior, Irlanda.

Sentencia de 15 de diciembre de 1983 emitida por el Tribunal Constitucional Federal Alemán. [Consulta 13-03-20]. Disponible en: http://www.informatica-juridica.com/jurisprudencia/alemania.asp.

165823. 1a. CCXIV/2009. Primera Sala. Novena época. Semanario Judicial de la Federación y su Gaceta. Tomo XXX, diciembre de 2009, p. 277. Derecho a la Vida Privada. [Consulta 10-03-20]. Disponible en: http://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/165/165823.pdf. Fecha de consulta: 20 de agosto de 2018.

Instrumentos jurídicos y tratados internacionales

Constitución Política de los Estados Unidos Mexicanos. Diario Oficial de la Federación el 5 de febrero de 1917. P. 17.

Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados

Ley Federal de Protección de Datos Personales en Posesión de los Particulares Tratado entre Estados Unidos de Norteamérica, Canadá y México en materia comercial. [Consulta 17-03-20]. Disponible en: https://www.gob.mx/t-mec

Capítulo 19 de Comercio Digital del TMEC. [Consulta 17-03-20]. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/465801/19ESPComercioDigital.pdf